

The Phenomenon of Unsolicited E-mails with Attachments

Xingan Li

University of Turku

ABSTRACT

Unsolicited e-mails became prevalent with the growing penetration of computer networks. The senders of unsolicited e-mails make every effort to get the attention of the recipient. The goal is for their messages and/or attachments to be opened. The victimization of recipients of unsolicited messages with attachments happens without the recipients actually accessing their e-mail accounts. The victimization-conspiracy model happens when the messages include contents offering products or services that need illegal involvement of the recipients. The recipients of messages with such offers are first victimized by the unsolicited messages; and if they accept the illegal services or purchase the illegal products, they are likely to become the co-conspirators of the senders. The senders and the recipient would reach an illegal double win effect. The unsolicited messages with attachments provide e-mail users many different options. The majority of messages in this study, however, offered recipients two alternatives; to conspire in tax evasion, or to be damaged by viruses.

Introduction

The open access of the Internet to commercial users at the end of the twentieth century created a new path to social life in this era. As of 2005, more than 683 million e-mail users hold 1.2 billion accounts (Radical Group, 2005), utilizing this unprecedented means of communication and marketing on a daily basis. Unsolicited e-mails have become a nuisance that every computer and internet user must deal with. The recipients' property rights, fair trade, public morals, cybersecurity, data protection, and other content-related and goods-related transgresses and offences are all challenges that society is confronted with (Li, 2006). The unsolicited e-mails can cause disruption of information transmission, commercial transaction, military operation, education, and recreation.

Many studies have been done to explore the phenomenology of unsolicited commercial e-mail (UCE, or unsolicited bulk e-mail, UBE, or simply spam). Others have dealt particularly with the costs and benefits for both senders and recipients that is derived from the unsolicited e-mail (Khong, 2001, 2004), the overall impact on productivity of individual employees and enterprises (Nucleus, 2003, 2004), the scale and volume of unsolicited e-mail (Radical Group, 2005), the impact on a consumers' attitude and their confidence towards e-commerce (TACD, 2003; Fallows, 2003; Harris Interactive, 2003), the higher possibility of receiving unsolicited e-mail due to online-published addresses (Federal Trade Commission, 2002b), the ignorance of removal requests by senders (Federal Trade Commission, 2002a), and the technical and legal solution on unsolicited e-mail (Sorkin, 2001).

Few studies, however, have dealt with unsolicited e-mails with attachments, particularly the degree of risk a single e-mail user might be confronted with. In this study, I use a sample of 501 unsolicited e-mails with attachments, first presenting the analysis of the types of sender column, types of subject column, types of offers in message content, and types, sizes and nature of attachments to these messages. Hereinafter the term "spam" is deliberately avoided by the author, due to the lack of a universally-accepted unified definition. The author prefers the phrase "unsolicited e-mail" without the modifier "commercial", in order to enlarge the coverage of messages with attachments in this study to virus spreaders.

Literature Review

The increased capability of computers and networks to process information, causes a "wealth of information" and can lead to "poverty of attention" (Simon, 1982). Unsolicited bulk e-mail

(UBE) or unsolicited commercial e-mail (UCE) represents an example of the superfluous information that e-mail users must deal with and do not expect to consume. Unsolicited e-mail brings about the negative image of e-marketing; frightening e-mail users from trusting e-mail communications.

Unsolicited e-mails sent to multiple recipients can have broad negative effects on e-mail marketing. An increasing number of e-mails are never read by the recipients, and the users prefer limiting or disrupting the business contacts (Karnell, 2002). The prevalence of unsolicited messages demonstrates a growing threat to the information society (World Summit on the Information Society, 2003, paragraph 37).

A few studies disclosed the spamming behaviour by narrative discourse about the reasons and methods of spamming, revealing the wisdom of defeating anti-spam techniques, avoiding being identified, and escaping the law (Spammer-X, 2004). Some also described the world of the spammers and spam-fighters, giving information on the mechanisms of spamming and spam fighting (McWilliams, 2005). Others presented the most usual spam traps and explained why the current solutions are ineffective (Goodman, 2004). Efforts have also been made to analyse a wide variety of e-mail in order to produce a profile of spam and develop a profile of the spammers (Lambert, 2003).

Unsolicited e-mails usually involve multiple scams. A dozen of the most likely spam scams have been identified. They cover spam and scams from business opportunities to quick money, working at home, guaranteed loans, and so on (Federal Trade Commission, 1998).

Besides direct victimisation, unsolicited e-mails have other indirect effects on productivity. An average of 13.3 unsolicited messages reached the employee per day; each employee then spent an average of 6.5 minutes per day dealing with the unsolicited messages. These unsolicited messages caused an average of 1.4 percent in productivity loss per employee per year, equal to an average cost of 874 dollars per employee per year (Nucleus, 2003).

Although it is difficult to measure the costs and benefits of spamming, if the benefits obtained from the spamming outweigh the cost, then the spammer will likely undertake the spamming activity (Khong, 2004). It follows that if there is one successful commercial transaction, the spammer can realize his or her benefit. The costs that are involved in spamming can be roughly estimated according to the costs of bandwidth, message sending, and obtaining of the recipients address. The costs of bandwidth and message sending are minimal. According to Sadowsky (2003, p. 55), the spammer can obtain users' e-mail address in the 13 situations. Obviously, the most convenient and least expensive way is to harvest e-mail addresses automatically with specific software. The software is also available from Internet, either being free of charge or with an inexpensive price.

The revenue of spammer from sending message has been found high in a few studies Goodman and Routhwaite (2004). The concept of "the parasitic economics of spam" was proposed, meaning that the act of sending a message costs the sender less than it costs all other parties impacted by the sending of the message (Cobb, 2003, p. 2).

The cost and benefit of the spamming can also be estimated. The costs created by spam can be far reaching. They include the waste of the users' time, bandwidth and storage, anti-spam solutions, and overloading at the mailbox (Gauthronet and Drouard, 2001). The average amount of time and money lost in processing a single message might not be significant. However, theoretically, the loss of time and money in aggregate in dealing with these messages might be huge (Li, 2006). Spam also induces costs of the bandwidth and storage, losses due to interruption of services, and anti-spam solutions (Gauthronet and Drouard, 2001). The interruption of service is unfortunate for both the provider and user causing losses in business and confidence. Worldwide revenue for anti-spam solutions will exceed 1.7 billion dollars in 2008 (IDC, 2005). If the e-mail address has ever been put on the institution's Web site, or personal homepage, it is highly possibly that the address will be harvested, sold, and abused by senders (Federal Trade Commission, 2003b).

Unsolicited e-mail is almost never useful or beneficial to the recipient. Based on data from previous studies, it is reasonable to conclude that the recipients of unsolicited e-mail are at risk for both monetary and psychological losses (Li, 2006).

Worse yet, the number of unsolicited e-mails are increasing. Users received an average of twice the number unsolicited messages from the previous year, with an average 3.1 percent of productivity loss in 2004. The ability of technical solutions to unsolicited messages became less effective (Nucleus, 2004).

A long-term side effect of increasing unsolicited e-mails is that they cause some e-mail users to use e-mail less, and trust the online environment less. Fear of unsolicited messages increased (Fallows, 2003).

Although many regulatory methods have been implemented, and some of the messages seem to follow the rules, most removal links or addresses were dead or did not function, attempts to send reply e-mail messages were also unsuccessful (Federal Trade Commission, 2002a).

About 66 percent of spam messages are fraudulent in the “from” or subject columns, or in the message itself (Federal Trade Commission, 2003a). These false advertisements might distort the normal market of goods and services, harm the normal trade order, or reduce consumers’ confidence (The Directorate General of Telecommunications Ministry of Transportation and Communications, 2005, pp. 6–7). The large volume of spam, malicious programs and malicious linkages contained in the messages, are the main threats (PC World, 2003).

Anti-spamming techniques that are inadequate and regulations that are ineffective, have created a phenomenon of unsolicited e-mails developed with spam techniques. Web pages, newsgroups, and chat room are all attractive to unsolicited message senders for harvesting e-mail addresses (Federal Trade Commission, 2002b). Spammers continue to harvest e-mail address posted on web sites, and to a much lesser extent, those posted on blogs and USENET groups. Masking email addresses when posting on web sites can substantially reduce the risk of harvesting (Federal Trade Commission, 2005). Many spammers send their messages by unauthorized use of other individuals or organizations’ accounts (Organization of Economic Cooperation and Development, 2004). E-mail address harvesting software can collect this information automatically from web pages (Boldt, Carlsson and Jacobsson, 2004, p. 8). Based on the discussions of spy ware and on the findings from the two experiments, spy ware has a negative effect on computer security and user privacy. Spy ware enables for the spreading of e-mail addresses that may result in the receiving of unsolicited e-mail (Boldt, Carlsson and Jacobsson, 2004, p. 4).

Most online adults reported that they received more spam compared with six months earlier. Only 14 percent have seen a decline in the volume of spam. A majority of respondents reported unsolicited messages to be annoying or very annoying (Taylor, 2003).

Much has been done about the phenomenon of unsolicited e-mail. In this systematic discourse, there is an apparent silence about specific messages with attachments. This study will not begin with a description of the importance of studying such messages, but will directly sketch an overall picture of this phenomenon. Attachments pose problems other than messages themselves and deserve more observation. This study is looking at unsolicited e-mails with attachments by analysing a sample. The following section will briefly introduce the methodology.

Methodology

This article presents a case study on unsolicited e-mails with attachments, analysing the sender column, subject column, content and attachments of these messages. The sample was composed of 501 messages with attachments in about 25,960 unsolicited e-mails in one e-mail account collected during a 12-month period from June 2005 to May 2006.

In analysing each message, it is necessary to establish a standard to categorise the messages into different types according to their sender column, subject column, content and attachments. The standard to

decide if the sender column is proper is the name format. Personal names composed of “first name” and “surname” are considered proper, regardless of their order. The name for an organization is also easy to judge by comparing the name in the sender column with what appears in the content. If they are consistent with each other, and are reasonable names, then, they are counted as proper.

The standard for deciding whether a subject column is proper has been loosely defined. Because there is only one message labelled with an “AD:” label, in strict sense all the subject columns of other messages are improper. However, the emphasis of this paper is not to coincide with the legal standard. Rather, it is focused on the analysis of the phenomenon of unsolicited e-mails with attachments. The message with “AD:” label and messages with words explaining the content or consistent with the content are regarded as proper. All other messages where the subject column is inconsistent with the content is considered improper.

The content is categorised according to the offers provided, including products, financial, adult, IT-related, health, scam and fraud, leisure, political, spiritual, and other. But in this sample, financial, adult, health, scam and fraud, leisure, spiritual offers are not as significant as many other studies revealed. They are put into “other services.”

Findings

Types of File Formats of Attachments

Out of 501 messages with attachments, three attachments were missing. Other attachments are comprised of 14 kinds of document formats. Nearly forty percent of the attachments are “zip” or “rar” format compressed files, mostly viruses, which represent the most severe threats to the e-mail users’ computer security. Approximately one third of the total attachments are files of various image formats, including “gif,” “jpg,” and “scr.” Another one third of the attachments are files of various document formats, including “chm,” “doc,” “htm,” “txt,” and “xls.” These two categories are relatively virus-free, but include annoying contents and hyper links. These three categories constitute more than 94 percent of all attachments. Another less frequent category is files in executable file formats, including “exe” and “com,” accounting for 4.4 percent of all attachments.

In these file formats, files with filename extensions of “zip” and “rar” are more dangerous. All the other files types can be “opened” with some kind of programs upon download and the contents can be read in the case of documents, viewed in the case of images, listened to in the case of audio, or simply ignored in the case of executable programmes which may involve greater danger than other files. But it’s well known that the types of original files included in compressed files have to be opened by uncompress programmes, and then the unzipped files can be opened by other application programmes. The real danger does not come from files other than “zip” and “rar” because if people know the real type of the original files they can determine whether or not to open the files. The “zip” and “rar” files are much more devious. In fact, files concealed with the filename extensions of compressed files are usually not compressed files, but are executable programmes. Therefore, when users execute the first step and they think they are unzipping the file, they are actually activating the malicious programme. In fact, most virus-spreading messages are camouflaged in this manner.

Table 1. Types of file formats of attachments

Type of file format	Number	Percentage
Compressed (*.zip and *.rar)	195	38.9
Text based (*.chm, *.doc, *.htm, *.txt, and *.xls)	142	28.3
Image based (*.gif, *.jpg, and *.src)	117	23.4
Executable (*.com and *.exe)	22	4.4
Other	25	5
Total	501	100

Table 2. Sizes of messages with attachments

Size	Number	Percentage
<100kb	446	89.0
100–200kb	11	2.2
>200kb	44	8.8
Total 23,765kb	501	100

In unsolicited e-mails with image attachments, the content of the e-mail is concealed in images and displayed in the messages, thus the sender avoids the detection and blocking by text-based filters. In some cases, attachments also contain animated images that make it more difficult for spam filters to work.

Sizes of Messages with Attachments

The average size of the messages with attachments was 47.44kb. Approximately 90 percent of the messages with attachments were smaller than 100kb. Only 2 percent of these messages are between 100–200kb. Nearly 9 percent of the messages are bigger than 200kb. In fact, about 285 messages, which constitute more than half of the messages with attachments, are smaller than 30kb. The messages with the sizes of 1kb and 2kb alone, account for more than 28 percent of the sample. They are mostly empty “zip” files, with the possibility of attachments containing viruses that may have been disinfected by the e-mail service provider. The messages with attachments spreading W32.netsky.C@mm (35kb) and W32.Sober.X@mm (75kb) viruses account for 16 percent and 7 percent of all of the messages respectively.

A majority of attachments are smaller than 200kb, a size that a majority of most dangerous viruses, worms, Trojan Horses, or other malicious programmes take. Most viruses are small in size, yet extremely harmful. That’s why they are so suitable to be spread by e-mail attachments.

Unsolicited messages with attachments account for less than 2 percent of all unsolicited messages. The average size of unsolicited e-mails with attachments is 47.44kb, compared with the average size of 7.32kb for other unsolicited e-mails, 6.5 times larger. In fact, unsolicited messages with attachments contribute to more than 10 percent of the average size of all unsolicited messages, enlarging the average size from 7.32kb of unsolicited messages without attachments to 8.09kb of all of the unsolicited messages.

Many people claim that unsolicited e-mails consume large amount of internet bandwidth. It is clear that messages with attachments are even more harmful than those without. Unsolicited e-mails with attachments are likely to cause even greater bandwidth problems. The increasing size and number of unsolicited e-mails will likely cause additional operating cost in server processing time and storage capacity.

Types of Sender Column in Unsolicited Messages with Attachments

Among the 501 messages with attachments, one had a blank sender column. Senders of unsolicited messages with attachments tend to hide their names but show their e-mail addresses, proper or not. Approximately 60 percent of all messages show e-mail addresses instead of the senders’ name, which should be considered improper. Others conceal their names with their surnames and titles, meaningless letters and numbers, describing their offers (products, services and activities), filled with words inducing users to open the messages, or simply exploiting recipients’ names and e-mail address. Approximately

Table 3. Compare of average sizes of messages

Item	Total size	Number	Average size
Average size of unsolicited e-mails with attachments	23,765kb	501	47.44kb
Average size of other unsolicited e-mails	186,254kb	25,459	7.32kb
Average size of all unsolicited e-mails	210,019kb	25,960	8.09kb

Table 4. Types of sender column in unsolicited messages with attachments

Type	Number	Percentage (/ 501)
Proper	124	24.8
Improper	377	75.2
Total	501	100

Table 5. High ratio of proper sender column in unsolicited message with attachments

Type of offer	Number of proper sender column	Percentage
Political	14	56
Quick money	1	50
IT related	33	70.2
Tax evasion	37	53.6
Employment	6	60

three quarters of the messages bear improper sender columns. About one quarter of the messages bear proper personal names or company names.

The improper sender columns include the following: blank, product descriptions, services and activities, meaningless letters and numbers, recipients' name and address, recipients e-mail address or surname plus title. These are all methods used to avoid showing sender names. As Khong (2001) pointed out,

“Because of flames and mail bombs from angered spam recipients, many spammers do not use valid email addresses in their spam. However, this causes difficulties for spam recipients to contact the spammers in order to request not to be spammed in the future.” (p. 24)

In different types of offers the proportion of messages with proper sender column are different. Messages providing political propaganda, quick money, IT related products and services, tax evasion and employment have a high ratio of formal sender column.

Table 6. Types of subject column in unsolicited messages with attachments

Type	Number	Percentage
Proper (with “AD:” label)	1	0.2
Improper	500	99.8
Pretending as contacts	202	40.4
Describing message content	117	23.4
Pretending as service provider	84	16.8
Misleading statements	74	14.8
Other	23	4.6
Total	501	100

Table 7. Types of content of messages with attachments

Type	Number	Percentage
Virus	141	28
Products	109	21.8
Empty attachments	103	20.6
Tax evasion	69	13.8
IT related	29	5.8
Political	25	5
Other services	25	5
Total	501	100

Table 8. Consistency of contents with attachments

Type	Number	Consistency number	Consistency percentage within the category
Virus	141	0	0
Products	109	95	87.2
Empty attachments	103	0	0
Tax evasion	69	69	100
IT related	29	24	82.8
Political	25	25	100
Employment	14	11	78.6
Other services	11	5	45.5

Types of Subject Column in Unsolicited Messages with Attachments

In order for the filtering techniques to automatically identify and block unsolicited e-mails, laws in some countries require that the senders use particular labels in the subject column. To label the subject column with “AD:”, “ADV:”, or any other kinds of regulatory means, however, is a legislative invention that has never been respected by senders of unsolicited messages. Only less than two in one thousand messages have fulfilled this requirement. Two in one hundred of the messages with attachments left the subject column blank. Approximately 15 percent of messages used misleading statements to confuse the recipients. All others attempted to draw recipients’ attention and attract them to open the messages, furnished the subject column with languages describing the content, giving greetings, appearing related to users’ e-mail service, bearing “Re:” and “Fw:” labels, or pretending to be the recipients friend, etc.

Proper Subject Column in Unsolicited Messages with Attachments

Almost all of the senders of messages with attachments offering information on human resources recruitment, companies or websites, publishing, printing, card manufacture, etc., sales of health products, clothes, and tax evasion displayed the proper subject column. A high percentage of providers of telecommunications services, sellers of books, VCDs, and DVDs, training information providers, quick money information providers, and providers of other services provided proper subject columns in their messages. All the senders of other messages were reluctant to provide proper subjects for their potential recipients.

Types of Content of Messages with Attachments

More than 28 percent of messages are designed to spread viruses. More than one in five offers various products. More than one in five contained empty attachments. Messages offering tax evasion services constitute about 10 percent. The messages offering telecommunications services, political propaganda, and other services constitute around 5 percent separately. Interestingly, there are rarely any messages containing attachments involving adult content, investment chances, sales of pirated software, or other common offers frequently mentioned in other studies.

Table 9. Types of contact method provided in unsolicited messages with attachments

Contact Method	Number	Percentage (/501)
Traditional communications	50	10
Telecommunications	451	90
E-mail address	113	22.6
Fax number	79	15.8
Instant online chat	52	10.4
Mobile phone	112	22.4
Telephone	145	28.9
Website	182	36.3

Table 10. Proper and improper sender and subject columns and content

Item	Character	Number	Percentage
Sender	Proper	100	20
	Improper	401	80
Subject	Proper	166	33.1
	Improper	335	66.9
Content	Proper	260	51.9
	Improper	241	48.1

Consistency of Contents with Attachments

Interestingly, most messages have a high percentage of content consistency. The exceptions are messages with empty attachments and messages with attachments that spread viruses. In both these cases, the senders bypass technical filters and artificial judgments using different methods.

Types of Contact Method Provided in Unsolicited Messages with Attachments

Because many unsolicited messages with attachments are spreading viruses, they generally provide no contact information. However, there are a few exceptions. Other messages included one or more kinds of contact methods in the message texts. Out of 501 messages analyzed, more than one-third of the messages provided hyperlinks to websites, while less than one-third provided telephone numbers. Both e-mail addresses and mobile phone numbers are preferred by more than 22 percent of senders. Fax numbers and physical addresses are included in about 16 and 10 percent of messages respectively. Instant online chat systems, such as MSN and QQ, are provided in 10.4 percent of messages.

Unsubscribe is nothing more than a decoration in unsolicited messages with attachments. Unsubscribe methods are only provided in 2.2 percent of the messages. The usual method is to provide a URL link at the bottom of the messages for the recipients to click on. In the opened links, the recipients can access web pages where they can choose to unsubscribe. Some unsubscribe methods require the recipients to send e-mails to specific addresses. The users of unsolicited messages in this study have never subscribed any of the messages with attachments. These messages can all be viewed as opt-out e-mails. Most of the unsubscribe methods do not work effectively. In extreme cases, the link simply connects the recipient to a webpage requiring a fresh registration. This gives the impression that the sender's real intent is to obtain the recipient's profile, not to unsubscribe them at all.

Improper Sender, Subject and Content Column

One in five of the unsolicited messages with attachments used a proper format in the sender column, one in three used proper subject column, and more than half provided proper content. However, only 58 messages had both proper format of sender and subject columns, and 293 messages had both improper sender format and subject column. Another 42 messages had the proper sender column format but they contained an improper subject column format, while 108 messages had an improper sender column format while utilizing a proper subject column format. The overall percentage of messages with improper subject or sender columns constituted 88.4 percent.

Conclusions

From the findings of this study, like in other unsolicited e-mails, the senders of unsolicited e-mails with attachments make every effort to gain the attention of the recipient. Their main goal is for their messages and/or attachments to be opened. Generally, they use informal, irregular and illegal forms of sender and subject columns, but ensure the contents are consistent with their real intent (except messages spreading viruses) to demonstrate their offers and continue their scams.

The surveyed messages with attachments prove that, except messages spreading viruses, they are relatively moderate in the sense of harmfulness of the contents, compared with the findings in previous studies which did not distinguish between messages with attachments from those without.

In principle, the victimization of recipients of unsolicited messages with attachments happens without the actual access of the recipients to their e-mail accounts. The victimization means that their e-mail accounts are being spammed, whether they open their accounts or not. Under current legal framework, the receiving of unsolicited messages is sufficient to constitute victimization.

The victimization-conspiracy model happens when the messages include contents offering tax evasion services, transaction of unauthorised duplicated software, transaction of falsified documents, and so on. The recipients of messages with such offers are first victimized by the unsolicited messages; and if they accept the illegal services or purchase the illegal products, they are likely to become the co-conspirators of the senders. This study does not cover further exploration into the practical effects of such conspiracy, but the messages provide potential risks for the recipients to engage in the activities.

Because the recipients of the unsolicited messages inducing conspiracy in an illegal activity would expect to benefit from the cooperation with the senders, the senders are more likely to send these kind of messages. The senders and the recipient would reach an illegal double win effect. This phenomenon will have a profound impact on the development of deviant behaviour.

In addition, the unsolicited messages with attachments provide e-mail users many different options, either legitimate or illegitimate, either to conspire or to be further victimized by attached viruses or pre-established scams. The majority of messages in this study, however, offered recipients primarily two alternatives: to conspire in tax evasion, or to be damaged by viruses, because the character of these two kinds of messages deserves special observation.

In the case of conspiracy in tax evasion, the senders always provide valid contact methods so as to induce the recipients to participate in the illegitimate operation. The offer seemingly aims to establish a trust relationship between service provider and clients. But the effect is that they form a conspiracy. The recipients have to react actively before they become the co-conspirators of the tax evasion activities. The process might involve repeated e-mail exchanges after the initial unsolicited message. Under these circumstances, the unsolicited messages might be transformed into literally valuable (but morally wrong and legally prohibited) information. Thus the recipients might be less likely to reject such messages. Such messages become the communication means for the trespassers and criminals, posing a great threat to the social control over illegal activities.

In the case of viruses attack, the senders exploit social engineering to induce the recipients to open the messages and subsequently the attachments, by blurring the sender, subject columns and falsifying the message contents and attachment names. These messages do not require replies from the recipients before they cause damage. They are also dangerous for the recipients in the sense that they are likely to destroy hardware and software, devastate human resources, and obstruct business.

It is noteworthy to point out that the scale of this study is minimal, but the object of the study is important. For a better understanding of this phenomenon to be achieved, future studies can do more: adopting a bigger sample, incorporating content analysis, and conducting interviews with victims and perpetrators.

I would like to thank the anonymous reviewers, who contributed comments and recommendations on the initial version of this paper, which led to its overall improvement.

COLUMBIA ONLINE CITATION: HUMANITIES STYLE

Xingan, Li. "The Phenomenon of Unsolicited E-mails with Attachments." *Studies in Media & Information Literacy Education*, 7.2 (2007).

<http://www.utpress.utoronto.ca/journal/ejournals/simile> (insert access date here).

COLUMBIA ONLINE CITATION: SCIENTIFIC STYLE

Xingan, L. (2007). The Phenomenon of Unsolicited E-mails with Attachments. *Studies in Media & Information Literacy Education*, 7(2).
<http://www.utpress.utoronto.ca/journal/ejournals/simile> (insert access date here).

BIOGRAPHICAL NOTE

Li Xingan is currently a LL.D. student at the University of Turku, Finland. He holds a LL.B. from Inner Mongolia University in Huhhot, and a LL.M. from China University of Political Science and Law in Beijing. His research interest involves the criminal phenomenon related to the information system.

AUTHOR CONTACT INFORMATION

Li Xingan
 University of Turku
 Faculty of Law
 20014 Turun Yliopisto
 Finland
 E-mail: xingan.li@yahoo.com

References

- Boldt, M., Carlsson, B., & Jacobsson, A. (2004). Exploring Spyware Effects. Retrieved 31 May 2006, from http://psi.bth.se/mbo/exploring_spyware_effects-nordsec2004.pdf
- Cobb, S. (2003). The Economics of Spam. Retrieved 31 May 2006, from http://www.spamhelp.org/articles/economics_of_spam.pdf
- Fallows, D. (2003, October). Spam: How It Is hurting E-mail and Degrading Life on the Internet. Retrieved 31 May 2006, from http://www.pewinternet.org/pdfs/PIP_spam_Report.pdf
- Federal Trade Commission (1998, July). Federal Trade Commission Names its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, *Federal Trade Commission Consumer Alert*.
- Federal Trade Commission (2002a, April). *Remove Me Surf*.
- Federal Trade Commission (2002b, November). *E-mail Address Harvesting: How Spammers Reap What You Sow*.
- Federal Trade Commission (2003a, April). *False Claims in Spam: A Report by the Federal Trade Commission's Division of Marketing Practices*.
- Federal Trade Commission (2005, November). *Email Address Harvesting and the Effectiveness of Anti-Spam Filters: A Report by the Federal Trade Commission's Division of Marketing Practices*.
- Federal Trade Commission. (2003b, June 15). *National Do-Not-E-mail Report to Congress*.
- Gauthronet, S., & Drouard, E. (2001). *Unsolicited Commercial Communications and Data Protection*. Brussels: Commission of the European Communities, Internal Market Directorate General.
- Goodman, D. (2004). *Spam Wars: Our Last Best Chance to Defeat Spammers, Scammers & Hackers*. New York, New York: SelectBooks.
- Goodman, J.T., & Rounthwaite, R. (2004). Stopping Outgoing Spam. In *Proceedings of the 5th ACM Conference on Electronic Commerce*, 17–24 May, ACM Press, 30–39.
- IDC (2005, February 24). Worldwide Revenue for Antispam Solutions to Reach Over \$1.7 Billion in 2008, IDC Reveals. *IDC - Press Release*.
- Karnell, J. (2002). Raising the Stakes in Permission Marketing. Retrieved 31 May 2006, from <http://www.onetooninteractive.com/resource/whitepapers/0003.html>
- Khong, W.K. (2001, October). The Law and Economics of Junk E-mails (Spam). Retrieved 31 May 2006, from <http://www.frg.eur.nl/rile/emle/Theses/Khong.pdf>
- Khong, W.K. (2004). An Economic Analysis of Spam Law. *Erasmus Law and Economics Review*, 1(Febuary), 23–45.

- Lambert, A. (2003, September). *Analysis of Spam*. Master of Science in Computer Science Dissertation. Dublin: University of Dublin.
- Li, X. (2006). E-Marketing, Unsolicited Commercial Electronic Mail, and Legal Regulations, *Webology*, 3(1), 2006.
- McWilliams, B. (2005). *Spam Kings*, Sebastopol: O'Reilly Media.
- Nucleus (2003). *Spam: The Silent ROI Killer*, Research Note D59.
- Nucleus (2004). *Spam: The Serial ROI Killer*, Research Note E50.
- Organization of Economic Cooperation Development (2004). *Second Organization of Economic Cooperation and Development Workshop on Spam: Report of the Workshop*.
- Organization of Economic Cooperation Development (2003). *Organization of Economic Cooperation and Development Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, Author.
- PC World (2003, August 29). Sobig May Be Working for Spammers. Retrieved 31 May 2006 from <http://www.pcworld.com/news/article/0,aid,112261,00.asp>
- Radical Group (2005). *The Radical Group, Inc. Release Q1 2005 Market Numbers Update*.
- Sadowsky, G., Dempsey, J.X., Greenberg, A., Mack, B.J., & Schwartz, A. (2003). *Information Technology Security Handbook*. The International Bank for Reconstruction and Development.
- Simon, H.A. (1982). *Designing Organizations for an Information-Rich World: Models of Bounded Rationality*. Massachusetts: Massachusetts Institute of Technology Press.
- Sorkin, D.E. (2001). Technical and Legal Approached to Unsolicited Electronic E-mail. *University of San Francisco Law Review*, Vol. 35, pp. 325–384. Retrieved 31 May 2006, from <http://www.sorkin.org/articles/usf.pdf>
- Spammer-X (2004). *Inside the SPAM Cartel*. Rockland, Massachusetts: Synergies Publishing.
- Taylor, H. (2003, 10 December). Spam Keeps on Growing. Retrieved 31 May 2006, from http://www.harrisinteractive.com/harris_poll/index.asp?PID=424
- Trans Atlantic Consumer Dialogue (TACD) (2003). *Consumer Attitudes Regarding Unsolicited Commercial E-mail (Spam)*.
- World Summit of Information Society (2003, December). *Declaration of Principles-Building the Information Society: A Global Challenge in the New Millennium*.